Client

Figure 5 further illustrates a client 114. As noted above, the client 114 may be a client in the traditional server-client network sense (further configured to operate according to the invention), or the client 114 may be a node in a peer-to-peer network. The client 114 is always a client in the sense that it receives courseware 400 or another service from at least one content server 110.

The client 114 includes operating system software and networking software 500 such as Windows 3.1, Windows 95, Windows 98, Windows 2000, or Windows NT software, Ethernet software, and/or other software discussed in connection with Figure 2.

The client 114 also includes a browser 502, such as a Microsoft Internet Explorer or a Netscape browser, through which courseware and/or other content 400 is presented to the user. In addition, the registration module may be browser-based or Oracle-based and browser-transported, so that any client 114 which supports an Internet connection and a Web browser 502 can be used to contact the registration server 108 to create a new user registration.

As previously discussed, the client 114 receives courseware and/or other content 400 from the content server 110. The content 400 may be provided in portions 504 which are defined in one or more of the following ways. First, portions 504 may be critical portions which have been treated for enhanced intellectual property protection as discussed elsewhere herein. Second, the portions 504 may be non-critical portions or a mixture of critical and non-critical portions, which are downloaded early in preparation for later presentation to the user. Early downloading may take advantage of the relatively low cost of telephone connections as opposed to other connections. Finally, content portions

504 may be a mixture of critical and non-critical portions such as episodes or chapters in a presentation, which are sent from the content server 110 to the client 114 in sequence as the user proceeds through the content 400 presentation.

Other components of the client 114, including the security manager 402, meter manager 406, and funds flow manager 308, are discussed elsewhere herein.

Methods Generally

Figures 6 and 7 further illustrate methods of the present invention. Figure 6 illustrates generally intellectual property license enforcement methods of the present invention, while Figure 7 illustrates operational methods of the system 100 from the perspective of a courseware user. Although particular method steps embodying the present invention are expressly illustrated and described herein, it will be appreciated that system and configured storage medium embodiments may be formed according to methods of the present invention. Unless otherwise expressly indicated, the description herein of methods of the present invention therefore extends to corresponding systems and configured storage media, and the description of systems and configured storage media of the present invention extends likewise to corresponding methods.

License Enforcement Methods

In describing Figure 6, an overview is provided first. Then the individual steps are revisited and discussed in greater detail. During an identifying step 600, at least one critical portion of the content 400 is identified; courseware is one example of the "work" referred to in the corresponding section of the '302 application to which the present

application claims priority. The critical portion is separated, encapsulated, encrypted, compressed, created and added, and/or otherwise treated to enable enhanced protection during a treating step 602.

At some later time, a user requests access to the treated content 400 during a requesting step 604. If the content is not already present on a local content server 110, it may be moved to such a server 110 during a step 606. The non-critical portion of the content may be downloaded to the user's location during an optional early downloading step 608.

The user's right to access the critical portion is verified during an authenticating step 610, a metering and monitoring step 612 is started, and the critical portion is then provided to the user during a monitored downloading step 614. If the ongoing or recurring monitoring step 612 detects a violation of the license, a disabling step 616 occurs to prevent or inhibit further use of the treated content. Total license fees based on the metering are calculated and charged during an accounting step 618. Each of these steps will now be described in greater detail.

During the identifying step 600, one or more critical portions of the content 400 are identified. The critical portions should be small enough for rapid treatment during step 602 and rapid downloading during step 614, but critical enough to make most users pay the license fees charged during step 618 rather than use only the non-critical portions. In a multimedia course, for example, critical portions might include executable files or the answers to interactive tests. If the executable is large, critical portions might be part of the executable such as a jump table or a proprietary dynamically linked library file needed to perform I/O operations. Critical portions may be preexisting elements of the content

400, or they may be created and inserted in the content 400. For instance, handshake code may be added to an executable to require periodic successful handshakes with a server 110; if the handshake fails, execution is aborted.

In content 400 that contains no executable computer code, but merely contains audio, visual or other data, critical portions could be initialization or synchronization information, or particular text or images that convey important information to a user or provide important entertainment value. Two of the many possible examples include a final scene of a mystery in which the murderer is revealed, and a checklist summarizing the main steps in a diagnostic technique being taught by courseware 400.

During the treating step 602, critical portions of the content 400 are treated to restrict their unauthorized use. Possible treatments include creating and inserting security codes, separating pre-existing critical portions so they are not downloaded with the non-critical portions, encrypting critical portions, compressing critical portions with a proprietary method (which effectively combines compression and encryption), and/or encapsulating critical portions. One form of encapsulation places the critical portion in a database table, such as a relational database table in a commercial database format used by Oracle, Sybase, Informix, or another familiar vendor. This has the advantage of making critical portions easier for the system 100 to track, and the advantage of hiding critical portions from unauthorized discovery by file system tools that rely on filenames, such as directory listing and directory search tools.

The requesting step 604 may be performed using user login procedures, courseware and/or content selection tools such as menus, and network communication means and methods familiar to those of skill in the relevant arts, including those discussed

above in connection with Figure 1 and/or Figure 2. The user may also be asked for an account password, a credit card number, or similar guarantee that the license fees for use of the content 400 have been or will be paid. During the requesting step 604, the user is also shown the license agreement terms and conditions, and is then asked to actively accept or decline being bound by the license agreement.

During a content moving step 606, content 400 may be moved from another content server 110 (which may reside in another network 200 or which may be a repository content server 110 as discussed herein) to the local content server 110 which serves the client 114 that is being used (or that will be used) by the user in question. This is accomplished as described in connection with the content movement manager 310.

Content 400 which requires significant download time can be loaded early during the step 608, at least in part, to minimize the delay experienced by users. As the cost of telecommunications services has remained largely constant over time, while the price of memory and computational power have doubled in cost-effectiveness about every eighteen months, the invention allows one to reduce or eliminate the serving of machine readable classes in real-time over the web or the Internet or from a file server. Instead, content 400 is downloaded during step 608 using telecommunications connections which are slow but relatively inexpensive and often billed according to a flat rate rather than connection time.

For instance, knowing that tomorrow is the first day of class in a new course, the multimedia sound and images in the course 400 could be downloaded by students during the night before the course 400 is presented. Critical portions such as the executable code, audiovisual synchronization, or order of presentation could then be downloaded on an as-needed-and-still-authorized basis the next day during step 614.

During the step 612, a timing meter is started in cases where the license fee is not a flat per-use fee but is based instead on the connection time. Monitoring and metering may be separate steps in other methods according to the invention; monitoring is concerned primarily with preventing unauthorized use, while metering is performed as a basis for calculating license fees. Regardless, a system according to the invention starts monitoring the connection 116 to ensure that the use is still authorized and to prevent attempts to obtain a complete copy of the content which is not protected by treatment of critical portions. In particular, initial or further downloading of critical portions during step 614 is not allowed (because part of disabling step 616 occurs) if the monitoring step detects any of the following conditions:

1. The user logged in is not an authorized user (step 604 authentication failed);
2. The user site is not at an expected, authorized network 200 (IP or LAN or MAC or Ethernet and/or socket or port) address; or
3. The user site 114 failed to return an expected periodic security handshake value.

With further reference to the treating step 602 and the monitoring and metering step 612, the present invention allows an intellectual property owner to insert a meter and/or security code into any information set, executable application, image, video, or other computer based work 400 containing intellectual property, and to require a permanent relationship between such works and the metering software 406 which is located on a machine 110 remote from the user site 114. The relationship is preferably simple, lowering the processor and bandwidth requirements of the network communication path 116 between the metering server 110 and the user's site 114. The relationship

ensures in most cases that a copy of the work 400 will not be fully available except for licensed time periods and at licensed user sites.

In some embodiments, the content 400 has embedded in it a time stamp, a date stamp, a copy stamp, an Internet Protocol ("IP") address stamp, and/or code enforcing a requirement that the treated content only execute or display on the client 114 CRT when the computer 114 receiving the copy is in a recognized relationship with the computer 110 which sent the course. This relationship is via a POTS line 116, or any telecommunications link 116 which provides constant or reliable presence.

A constant or reliable presence allows a handshake once per configurable time interval or configurable repeated event. The handshake verifies that the user computer 114 in contact with the server 110 is still the same user computer 114, using its IP address or the IP address of its gateway and the password into the gateway required by its Internet service provider. On a local area network 200, the handshake may use the LAN address.

In some embodiments, in addition to the consistent verification that the content 400 is resident on the same user computer 114 connected via the same Internet service provider gateway IP address, both the server 110 with the meter 406 and the computer 114 with the content 400 have identical "random" number generators. These random or pseudo-random numbers must match each interval, or at least be in the same order (it is understood that the content recipient computer 114 may be hundreds of milliseconds away from the server 110 when a connection required for a course 400 travels over part of the Internet).

The random number pairing is once per client-server pair 114, 110; per workstation 114; or per connection 116, depending on the embodiment. In one embodiment,

for example, each connection 116 spawned from a content server 110 will have the same random paired number set. One set runs on the server 110, and the same set runs on each user computer 114 which is receiving the content 400 essentially simultaneously. To confirm that the sequence is the same, each computer 110, 114 has a date/time stamp program 402 running, and each date/time stamp must agree at least once per minute. Thus, any computer 114 presenting a course 400 in this way must reset its date/time clock to agree with the content server 110 date/time stamp.

In addition to, or instead of, metering content executables, the present invention can also meter "data transfer executables". Examples of data transfer executables include applications used to operate or access video conferencing cards, network interface cards, CD-ROM controllers, fax systems, modems, and other data transfer devices that can be used in multimedia, audio, or video presentations. For instance, the use of codec (compression – decompression) software and/or hardware which is used to transfer audio or visual data between data formats can be metered according to the invention.

Such metering and authentication systems and methods allow any course 400 to be downloaded to the personal computer 114 of the person who will be taking the course 400. The user's computer 114 may be located at the user's place of employment or at the user's home or at a training facility. An external hard drive can be rented with the course 400 and authentication software mounted. This hard drive can be connected to a personal computer 114 running Windows 95, Windows 2000, Windows NT, Macintosh, or other familiar operating system software, via comm port one or the like (WINDOWS 95, WINDOWS 2000, and WINDOWS NT are marks of Microsoft; MACINTOSH is a mark of Apple). Any personal computer user not needing additional hard drive space can

simply make an FTP request, set up the request before going to bed, and find the course 400 (or most of it if critical portions are not available for early downloading) available in the morning. By having much or all of the course 400 available on his or her personal computer 114, much or all of the course 400 will run at the speed of the backplane of that computer 114, which is often substantially faster than an Internet or other network link 116 transfer rate.

In one embodiment, the only information going back and forth via the Internet or via a POTS line connection 116 to the server 110 will be handshaking such as repeats of the IP address of the gateway, pinging, and a stream of paired random numbers to authenticate that the content 400 was obtained from this server 110. The name and password of the student will be sent each minute (or other predetermined interval) as well. Thus, each minute an IP address is sent, a name, a password, and a sequence of paired random or quasi-random numbers. In well under one kilobyte of communication data, the content 400 will be authenticated for another interval of use. As noted, the present invention provides the ability to disable the courseware or other content 400 on the student's personal computer 114 whenever the link 116 with the content server 110 is broken or lost.

To assist in the apprehension of someone who attempts to violate the security system of the present invention, the security system will record where the copy was obtained. A series of copy locations hidden in the content 400, or similar digital watermark information, maintain a record of IP gateway information, password information, and user ID information on how the copies were made, what order the copies were made in, and the time and date stamp of each copy of the content 400. The

information can be maintained in a circular buffer holding N records, with information for the N-plus-first copy being copied over the information related to the first copy so that the buffer file size remains the same.

User View of Operational Methods

Figure 7 illustrates methods for operating the architecture 100 from the point of view of a user. During a registering step 700, the user sits down at a client 114, locates the service provider Web site which is hosted by the registration server 108, and then provides registration information to the registration manager 300. Suitable registration information may include, for instance, the user's name, address, sponsor, password (the password may also be generated by the registration manager 300 rather than be provided by the user), and payment information such as a purchase order number or credit card number.

The registration manager 300 verifies that the username and password are unique by checking the database 302, and then adds a new user registration record to the database 302. Finally, the registration manager 300 notifies the user that registration is complete. If a sponsor was identified by the user, the registration manager 300 optionally also notifies a course administrator at the sponsor by email.

During an optional reserving step 702, the registered user reviews menus of available content and associated times and locations, and places one or more reservations with the reservation manager 304. The reservation manager 304 verifies availability and enters the reservation, using the reservations database 306. If a reserved course is

subsequently canceled, some embodiments of the reservation manager 304 send a notice to the registered user by email.

During a payment authorizing step 704, the registered user provides credit card information, and provided implicit or explicit authorization to bill the credit card for services provided. As noted above, this step may be part of the registering step 700. The payment authorizing step 704 may also be performed later, if the necessary information was not available at the time of beginning registration, for instance, or if the user wishes to identify a different credit card after initially registering.

More generally, the method steps illustrated in the Figures and discussed in the text may be performed in various orders, except in those cases in which the results of one step are required as input to another step. For instance, a user must be registered in order to view courseware 400 except to the extent that a particular embodiment provides demonstration courseware at no charge to unregistered users. Likewise, steps may be omitted unless called for in issued claims, regardless of whether they are expressly described as optional in this Detailed Description. For instance, users who are sponsored by a corporation or agency need not provide credit card information during a step 704. Steps may also be repeated (e.g., running several courses), or combined (e.g., providing credit card information during registration), or named differently (e.g., running a course may be referred to as "receiving services").

During a login step 706, a registered user logs into the content server 110. The initial login step 706 may be performed automatically when the user first registers during step 700. Later login steps 706 may be performed each time the user begins a new session at a client 114. During the login step, the user provides a username and password to the

security manager 402, which verifies that the corresponding user record exists in the registration database 302 replica on the content server 110.

In addition, if the user has indicated that payment will be by credit card, then the funds flow manager 308 checks the credit card and places a hold on the credit card for an amount which may depend on the prior history of the user, the user's sponsor, the courseware 400 requested, and similar information. In some embodiments, users are not allowed to complete the login process 706 unless the payment information provided by the user or by the user's sponsor has been accepted as valid by the funds flow manager 308.

A user may wish to bill part of a sitting to one account, such as an individual account or a particular employer, and bill a second part of the same day's training to a second account. This may be achieved by logging in under the first account, receiving the first part of the desired services, logging out, and then logging in again with a different user ID and/or password before receiving the second part of the desired services.

During a selecting step 708, the user may select one or more courses 400 to be presented at the client 114. In some cases, the course selection will already have been made by the user's sponsor. Courses 400 may be selected using menus and/or other user interface tools and techniques familiar in the art, which contain course 400 description, cost, and availability data copied from the reservation database 306.

During a step 710, the course 400 is presented to the user at the client 114. This involves sending courseware content 400 from the local content server 110 to the client 114 for viewing during a step 712 by the user. It may also include interaction between the user and other users and/or an instructor during a step 714. Interaction may be provided, for example, by using email, chat rooms, live audio, and/or live video carried over the

network connection(s) 116. In addition, during an optional step 716 the user may take one or more interactive tests or quizzes. These may be graded by courseware 400 which is resident on the workstation 114, or the user responses may be transmitted to the content server 110 for grading there, with the results then being sent back to the client 114 and/or to the instructor.

Presentation of courseware during step 710 may be interrupted by a step 718 in response to a key press, mouse click, or other action by the user. For instance, the user may decide not to continue the remainder of the presentation 400 at the present time, or may wish to terminate this presentation and start viewing a different course 400. The user may also simply want to take a temporary break, and then resume the presentation during a subsequent step 720.

During a step 722, the user receives an invoice for services rendered. This may be done in conjunction with a logout during step 722, or logging out may be delayed until a step 726 in which the invoice is paid. From the system's point of view, once a user decides to log out, the meter manager 406 completes the database 408 time table for the user ID, including each event ID associated with each courseware offering, test offering or other service provided during the session. The funds flow manager 308 then uses the database 408 time table and the database 408 rate table to present an invoice on the computer screen in the browser 502.

The user may accept or decline the stated invoice. If the user accepts the invoice, the funds flow manager 308 in the content server 110 communicates that acceptance to the funds flow manager 308 in the registration server 108, which in turn contacts the bank

to clear the hold previously placed during step 702, 704, 708 and have the bank apply the credit card charges to the user's card.

If the user declines the invoice, the user may seek an invoice adjustment during a step 724. The local network 200 administrator tries to answer any questions the user has about the invoice and to obtain user acceptance of the invoice, possibly after an adjustment. The local network 200 administrator or other local site personnel are authorized to make adjustments to the bill during step 618. A new invoice amount will then be passed to the funds flow manager 308 for credit card or other payment activity based on the payment terms presented during user registration and this particular session, and the results of any adjustment discussions.

Additional Comments on Security

In the architecture 100, security may be provided in several ways including those expressly noted above. Allowing one and only one person to have a given user ID helps ensure that persons who use content 400 are properly billed for such use, as noted above. But in addition, the user ID and the credit card information help protect the reservation module. If reservations were available without a credit card hold or similar protection, a malicious user could reserve seats in a network 200 (or even reserve all seats in the entire architecture 100) with no legitimate intent to use them. By requiring a credit card for reservation, the reservation module is protected because adequate credit must be available to pay for all reservations placed.

Because content is not stored on the registration server 108, security precautions can be taken that might not otherwise be available. For instance, access to the home page

can be disabled so that outsiders cannot input messages or modify HTML code on the registration server 108. Dynamically produced Web pages based on information provided by the user, and created by Oracle or similar software, are also more difficult to modify than static HTML pages. Firewalls, encryption, and other means can also be used to protect credit card numbers of users in time-limited secure transactions without reducing security to allow continual courseware 400 usage from the same server 108. In one embodiment, the registration server 108 exports credit card information to other servers with heightened security; once the export is complete, the credit card information is deleted from the registration server 108.

Summary

The present invention provides systems, devices, and methods for technical enforcement of intellectual property right agreements. A security enforcer is inserted into deliverable content, or a small but critical portion of the content is treated to make it unusable without authorization (unable to execute, for instance), or both treatments are performed. A relationship over time is created between a meter and the treated (secured) content; without the relationship, use of the content is hindered or disabled. The critical portion is never placed in a user's persistent (nonvolatile) storage, such as a disk or tape storage, or alternatively is never placed in persistent storage in usable (executable, runnable, viewable, legible, audible) form. At least part of the meter is remote from the user, being located on a network server 110 while the user uses a client computer 114. The meter is made unique to the content server 110, through the use of IP addresses, coordinated random numbers, and the like. The meter stops running, and the content

stops being fully usable, if the client 114 is disconnected for longer than a predetermined period or if the security handshake fails for some other reason.

As used herein, terms such as "a" and "the" and item designations such as "client" are inclusive of one or more of the indicated item. In particular, in the claims a reference to an item means at least one such item is required. When exactly one item is intended, this document will state that requirement expressly.

The invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. Headings are for convenience only. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by patent is:

1. A multi-level computer architecture for managing content in a shared use operating environment, the architecture including:

a registration server level including at least one registration server, each registration server comprising a remote registration manager and a registration database for new user registration, and each registration server being further characterized in that it is free of content managed by the architecture;

a content server level including at least one content server, each content server linked for network communications with a registration server, each content server containing content managed by the architecture, and each content server being further characterized in that it serves such content only for presentation to registered users, namely, users who have previously been registered with a registration server; and

a client level including at least one client workstation, each client workstation connectable to a content server by a client-server network communications link, and each client workstation being further characterized in that it presents to at least one registered user content which is served over the client-server network communications link by the content server.

2. The computer architecture of claim 1, wherein the content comprises courseware.

3. The computer architecture of claim 1, wherein the registration server further includes a reservation manager and a reservation database which permits registered users to reserve content.

4. The computer architecture of claim 3, further comprising a funds flow manager for managing payment information, wherein the reservation manager, the reservation database, or both, operate with the funds flow manager to provide registered users with guaranteed content reservations.

5. The computer architecture of claim 1, further comprising a funds flow manager for managing content usage payment information.

6. The computer architecture of claim 5, wherein a portion of the funds flow manager resides on each client workstation, a portion resides on each content server, and a portion resides on each registration server.

7. The computer architecture of claim 1, further comprising a security manager for preventing unauthorized use of the content.

8. The computer architecture of claim 7, wherein a portion of the security manager resides on each client workstation and a portion resides on each content server.

9. The computer architecture of claim 7, wherein critical portions of the content reside in database tables managed by the security manager.

10. The computer architecture of claim 7, wherein the security manager is further characterized in that it sends at least part of a critical portion of content only to a volatile client workstation memory rather than sending it to a nonvolatile client workstation memory.

11. The computer architecture of claim 1, wherein each content server further comprises a launch manager for launching presentations of courseware content.

12. The computer architecture of claim 1, further comprising a meter manager for metering content usage.

13. The computer architecture of claim 12, wherein a portion of the meter manager resides on each client workstation and a portion resides on each content server.

14. The computer architecture of claim 1, wherein each client workstation comprises a web browser through which content is presented.

15. The computer architecture of claim 1, further comprising a backup registration server containing data mirrored from the registration server.

16. A method for managing content in a shared use operating environment, the shared use operating environment including a registration server, a content server connectable by a network link to the registration server, and a client workstation connectable by a client-server network communications link to the content server, the method comprising the steps of:

registering a user at the registration server, thereby characterizing the user as a registered user;

receiving at the content server a request by the registered user for access to content which contains at least one previously treated critical portion;

authenticating the request;

serving at least the critical portion over the client-server network communications link for presentation to the registered user at the client workstation; and

metering usage of the content by the registered user.

17. The method of claim 16, further comprising the step of treating the critical portion, thereby enabling enhanced intellectual property right protection of the content by technical means.

18. The method of claim 17, wherein the treating step comprises inserting disabling code into an executable portion of courseware content.

19. The method of claim 17, wherein the treating step comprises encapsulating the critical portion in a database table.

20. The method of claim 16, further comprising the step of downloading at least one non-critical portion of the content to the client workstation at least two hours before serving the critical portion.

21. The method of claim 16, further comprising the step of monitoring the client-server network communications link.

22. The method of claim 21, further comprising the step of disabling use of at least a portion of the content after an expected security handshake is not received.

23. The method of claim 16, further comprising the step of disabling caching and other disk writes to prevent a copy of the critical portion of the content from being created on nonvolatile storage at the client workstation.

24. The method of claim 16, further comprising the step of presenting the registered user with an invoice for usage of the content.

25. The method of claim 24, further comprising the step of allowing a local administrator to adjust the invoice presented to the user in response to a request by the user for an adjustment.

26. The method of claim 16, further comprising the step of obtaining a credit card payment authorization to permit payment by credit card for usage of the content.

27. The method of claim 16, further comprising the step of reserving a particular piece of courseware content for a particular registered user.

28. A computer storage medium having a configuration that represents data and instructions which will cause at least a portion of a multi-level computer system to perform method steps for managing courseware in a shared use operating environment, the shared use operating environment including a server and a client connectable by a network communications link to the server, the method comprising the steps of:

receiving at the server a request by a registered user for access to courseware which contains at least one previously treated critical portion;

serving at least the critical portion over the network communications link for presentation to the registered user at the client; and

monitoring the network communications link to prevent unauthorized use of the courseware.

29. The configured storage medium of claim 28, wherein the method further comprises the step of treating the critical portion, thereby enabling enhanced intellectual property right protection of the courseware.

30. The configured storage medium of claim 29, wherein the treating step comprises inserting disabling code into an executable portion of the courseware.

31. The configured storage medium of claim 29, wherein the treating step comprises encapsulating the critical portion in a database table.

32. The configured storage medium of claim 28, wherein the method further comprises the step of downloading at least one non-critical portion of the courseware to the client at least one hour before serving the critical portion.

33. The configured storage medium of claim 28, wherein the method further comprises the steps of metering usage of the courseware and charging for metered usage.

34. The configured storage medium of claim 28, wherein the method further comprises the step of disabling disk writes to reduce the risk that a copy of the critical portion of the courseware will be created on nonvolatile storage at the client.

35. The configured storage medium of claim 28, wherein the method further comprises the step of presenting an invoice for usage of the courseware.

36. The configured storage medium of claim 35, wherein the method further comprises the step of allowing a local administrator to adjust the invoice presented.

37. The configured storage medium of claim 28, wherein the method further comprises the step of reserving with a guarantee a particular piece of courseware for a particular user.